[19]中华人民共和国国家知识产权局

[51]Int.Cl[7]
H04Q 7/24
H04L 29/06

[12]发明专利申请公开说明书

[21]申请号 99110376.9

[43]公开日 2000年3月8日

[11]公开号 CN 1246773A

[22]申请日 1999.7.16 [21]申请号 99110376.9
[30]优先权
[32]1998.7.17 [33]US [31]09/118,640
[71]申请人 电话通有限公司
地址 美国加利福尼亚州
[72]发明人 廖汉青 彼得·F·金
小布鲁斯·K·马丁

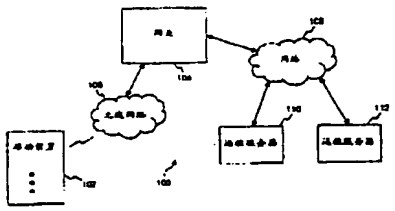
[74]专利代理机构 柳沈知识产权律师事务所
代理人 马莹

权利要求书 3 页 说明书 16 页 附图页数 10 页

[54]发明名称 提供对移动装置本地服务的访问控制的方法和装置

[57]摘要

公开了一种保证安全访问无线通信系统的移动装置的本地服务的技术。该技术 控制访问移动装置的本地服务,以使仅有授权的服务能够远程更改该本地服务 。在允许访问本地服务之前,检验寻求访问的网点身份,以判断该网点是否被 授权了这样的访问。如果网点为授权的,则允许访问,并且网点能够修改或更 改移动装置的本地服务。另一方面,当网点为非授权的时,拒绝该网点访问本 地服务,以使网点所提供的本地服务不受到未经意的网点的破坏。



ISSN1008-4274

权 利 要 求 书

1. 一种用于限制访问一移动装置的本地服务的方法，所述方法包括:

(a) 通过一网络接收来自一计算装置的消息，该消息具有与其有关的服务标识;

(b) 判断所述消息是否寻求对所述移动装置的本地服务的访问;

(c) 至少当所述判断步骤(b)判断出所述消息寻求对所述移动装置的本地服务的访问时，将与所述消息有关的服务标识与一个或多个授权的服务标识进行比较; 和

(d) 仅当所述比较步骤(c)表明与所述消息有关的服务标识与至少一个或多个授权的服务标识相匹配时，允许所述消息访问所述移动装置的本地服务.

2. 如权利要求 1 所述的方法，其中所述本地服务属于提供在所述移动装置上的服务.

3. 如权利要求 1 所述的方法，其中所述消息包含可执行代码.

4. 如权利要求 3 所述的方法，其中所述允许步骤(d)包括: 当与所述消息有关的服务标识与至少一个名多个授权的服务标识相匹配时，处理所述消息.

5. 如权利要求 1 所述的方法，其中所述消息的服务标识属于提供该消息的网络上的所述计算装置.

6. 如权利要求 1 所述的方法，其中所述消息的服务标识是通用资源定位器.

7. 如权利要求 1 所述的方法，其中所述消息的服务标识是从域名推导出的一串、一通常资源定位器、一网络地址、一字母数字文本串和一电话号码.

8. 如权利要求 1 所述的方法，其中所述判断步骤(d)进行操作，以扫描所述消息的至少一个部分，从而判断所述消息是否寻求对所述移动装置的本地服务的访问.

9. 如权利要求 1 所述的方法，

其中所述消息包括可执行代码，该可执行代码使所述本地服务被处理，以使所述移动装置中的存储的系统参数被修改，从而更改所述移动装置的操作，并且

服务提供器可规定移动装置改变由该移动装置支持的本地服务参数. 结果，移动装置的本地服务容易受到来自黑客(hacker)的恶意攻击等以及其它可使移动装置不能操作或在不需要的状态下操作的类似事件. 例如，可从未经意的远程服务器将病毒代码不需要地下载到移动装置，结果擦除或破坏了当前存储在移动装置中的本地服务参数，使移动装置不再能正确操作.

这样，就有了对保证安全访问移动装置的本地服务参数的需求.

广义上来讲，本发明涉及限制访问移动装置的本地服务的技术. 本地服务的功能包括: 修改无线话音/数据协议、配置或系统参数、书签(bookmarks)、地址、客户规定信息和可以使移动装置的某些通话和数据特征有效或无效的其它参数. 移动装置包括(但不限于): 移动计算装置、蜂窝电话、掌上型计算机装置和个人数字助理(Personal Digital Assistant, PDA). 移动装置能够与网络上的一个或多个服务提供器或远程服务器进行无线通信. 本发明提供对移动装置的本地服务的安全访问，以使仅有授权的服务(例如，来自授权的服务器或网点)能够远程调用或更新移动装置的本地服务. 按照本发明，在允许访问移动装置的本地服务之前，检查寻求访问的远程服务的身份(identity)，以判断该远程服务是否被授权了这样的访问. 如果该远程服务为授权的，则允许访问，并且该远程服务能够执行或更新移动装置的本地服务. 相反，如果远程服务为非授权的，则拒绝访问，以使移动装置所提供的本地服务不易受到来自未授权的远程服务的攻击或破坏，这些未授权的远程服务来自未经意的服务器或网点.

本发明能够以多种方式来实施，包括方法、计算机可读介质、设备和系统. 下面将讨论本发明的几个实施例.

作为保证安全访问移动装置的本地服务的方法，本发明的一个实施例包括步骤: 通过一网络接收来自一计算机的消息，该消息具有与其有关的服务标识(identity); 判断所述消息是否寻求对所述移动装置的本地服务的访问; 至少当判断步骤判断出所述消息寻求对所述移动装置的本地服务的访问时，将与所述消息有关的服务标识与一个或多个授权的服务标识进行比较; 以及，仅当所述比较步骤表明与所述消息有关的服务标识与至少一个或多个授权的服务标识相匹配时，允许所述消息访问所述移动装置的本地服务.

作为具有计算机程序代码的计算机可读介质，所述计算机程序代码用于保证安全访问一移动装置的本地服务，本发明的一个实施例包括: 用于通过

图 2 是根据本发明的一个实施例的移动装置初始化处理的流程图;

图 3A 和 3B 是根据本发明的一个实施例的移动装置消息处理的流程图;

图 4A 和 4B 是根据本发明的另一个实施例的移动装置消息处理的流程图;

图 5 是根据本发明的一个实施例的网关处理的流程图;

图 6 是用于本发明的典型通信系统的方框图;

图 7A 是适用于图 6 所示的典型通信系统的网关的方框图; 和

图 7B 是适用于图 6 所示的典型通信系统的移动装置的方框图。

本发明涉及用于保证对一无线数据网络的移动装置的本地服务的安全访问的技术. 本发明提供控制访问移动装置的本地服务(例如, 本地服务参数)的技术, 以使仅有授权的服务(例如, 授权的网点)能够远程改变移动装置的本地服务. 本发明因此能防止未授权的服务(例如, 黑客或未授权的网点)改变移动装置的本地服务.

下面将参照图 1 - 7B 讨论本发明的实施例. 然而, 本领域的技术人员容易理解, 这里对于附图所给出的详细解释仅仅是为了说明的目的, 本发明的范围远远超出这些有限的实施例.

图 1 是根据本发明的实施例的无线通信网络 100 的方框图. 无线通信网络 100 包括一移动装置 102, 该移动装置 102 通过无线网络 106 与一网关(或代理服务器)104 通信. 网关 104 也耦合到网络 108 . 网络 108 可以是专用网络(private network)或公共网络, 可以是有线的也可以是无线的. 大型公共网络的例子是因特网. 网络 108 包括或耦合到多个远程服务器, 包括远程服务器 110 和远程服务器 112 .

网关 104 通常是计算机系统, 该系统进行操作, 以将信息发送到移动装置 102 和网络 108 并且从移动装置 102 和网络 108 接收信息. 虽然在图 1 中仅示出了一个移动装置 102 , 应当认识到, 无线通信网络 100 可以容纳巨大数量的移动装置. 无线网络 106 通常使用无线传输, 以便与移动装置 102 通信. 无线网络 106 可以使用许多不同的网络和通信协议. 无线网络比如包括(下面列举一些)蜂窝数字分组数据(CDPD)、全球移动通信系统(GSM)、码分多址(CDMA)和时分多址(TDMA), 每一个这些无线网络具有不同的数据传送特性, 比如等待时间、带宽、协议和连接方法. 例如, 协议可以是因特网协议(IP)、短消息系统(SMS)和未构造的补充服务数据(Unstructured

Supplementary Service Data, USSD)，并且连接方法可以包括分组切换或电路切换.

远程服务器 110 和 112 通常为耦合到网络 108 的计算机. 通常，服务器提供通过网络 108 可访问的资源. 这些远程服务器 110 和 112 可提供的一种服务是用于移动装置 102 的规定信息. 换言之，移动装置 102 可访问远程服务器 110 或远程服务器 112，以提取使移动装置 102 通过无线被规定的规定信息. 例如，在移动装置 102 事先规定为以 CDMA 方式操作的情况下，当远程服务器 112 检测到移动装置 102 处于 CDMA 不再有效的位置时，现在由远程服务器 112 中的授权的服务规定为以 CSM 方式操作. 通常，由授权的服务通过特定的远程服务器对移动装置 102 进行的规定，可提供移动装置 102 上的服务，这些服务对应于所述远程服务器或其上属(owner)或分支所提供的服务. 用于规定移动装置 102 的规定信息通常作为从远程服务器 112 或 110 发送的消息或者由移动装置 102 请求的消息获得. 最好，提供信息的格式是可在无线网络 106 中最有效地传输的格式. 有许多不同的格式，比如 ASCII数据、二进制数据、可执行或目标代码，每一种格式都适用于一特定的无线网络. 根据一个实施例，该格式是可执行代码. 在接收到可执行代码中的规定信息时，移动装置 102 执行随后使移动装置被相应规定的可执行代码. 在一个实施例中，可执行代码包括一个或多个压缩的手持设备标记语言卡片组(Handheld Device Markup Language Decks)或 HDML 卡片组. 每一个卡片组包括多个卡，每一个卡对应于移动装置的屏幕显示. 或者，移动装置 102 的用户可以提供有屏幕显示中的列表选项，以执行或更新想要的本地服务. HDML 的规范，题为“HDML 2.0 语言基准”，在此通过引用其全文而将其包括并纳入此文.

例如，用于移动装置的一个本地服务可以是电话簿. 为使用电话簿，移动装置将访问远程服务器，以获得用于使用电话簿的规定信息，或者在用户执行命令之后更新电话簿中的信息. 通常，规定信息是可下载和可执行的可执行代码，并随后使用移动装置上的本地服务，以建立使用电话簿的移动装置. 规定信息也可以包括电话簿或者其汇接局(link).

如上所述，传统的无线通信网络不提供对其移动装置的本地服务的保护. 换言之，可对移动装置的本地服务进行非授权的访问. 结果，通过规定移动装置，未经意的人们可以使移动装置不能操作或变得无用. 例如，黑客

可以通过本地服务的远程调用将病毒植入移动装置.

根据本发明，移动装置仅允许某些远程服务访问该装置的本地服务，使该装置修改或更新系统参数，以使该装置相应地进行工作．以这种方式，本地服务得到了安全保护，不会受到未授权的干扰，这些未授权的干扰可导致不可操作性或移动装置的有价值信息的不可恢复的损失．本发明的操作提供对本地服务信息的这种保护，下面将讨论本发明的操作．

图 2 是根据本发明的一个实施例的移动装置初始化处理 200 的流程图．移动装置初始化处理 200 是由移动装置执行的，该移动装置比如为图 1 所示的移动装置 102 .

移动装置初始化处理 200 首先在移动装置 102 和网关 104 之间建立安全连接(步骤 202)．执行在移动装置和网关之间的安全连接(或对话)的建立，以使移动装置与网络上的远程服务器(例如，网络 108 上的远程服务器 110 和 112)安全通信．通常，由于是专用网络而使得这种连接是安全的，或者，这种连接是通过加密来使其安全的．于是，一旦建立了安全连接，就可从网关 104 将包括授权的服务标识的规定信息和其它安全数据下载到移动装置 102(步骤 204)．所述安全连接防止了随后在网关 104 和移动装置 102 之间传送的信息被截取或更改．建立安全连接或通信对话的另外的详细描述提供在共同转让的美国专利申请 No. 08/966,988 中，该专利申请的题目为“在无线数据网络中进行安全轻松的事务处理的方法和系统(Method and System for Secure Lightweight Transactions in Wireless Data Networks”，由廖汉青等人所著，该申请在此参照其全文而包括在此文中．在步骤 204 之后，完成并结束移动装置初始化处理 200 .

图 3A 和 3B 是根据本发明的一个实施例的移动装置消息处理 300 的流程图．该移动装置消息处理 300 例如是由图 1 所示的移动装置 102 执行的．因为消息通常是从网络提供给移动装置的任何数据块，在通过无线规定移动装置的情况下，消息通常包含要由移动装置上执行的可执行代码．由移动装置对可执行代码的执行可调用实际进行该移动装置的规定的该装置的本地服务．可执行代码的格式的变化很广，包括脚本、 JAVA 、 HDML 卡片组、ASCII数据、库函数等．

移动装置消息处理 300 首先以确定步骤 302 开始，该步骤判断是否从网络接收了一消息．例如，来自网络的消息可以通过网关提供给移动装置．只

要确定步骤 302 判断出还没有从网络接收到消息，则移动装置消息处理 300 等待接收这样的消息．然而，一旦已从网络接收到消息，则移动装置消息处理 300 继续．

一旦移动装置消息处理 300 继续，则确定步骤 304 判断该消息是否请求本地服务访问．这里，确定步骤 304 判断已从网络接收的消息是否请求对移动装置的本地服务的访问．对本地服务的访问意味着调用移动装置所提供的本地服务，该访问可以修改(例如，增加、删除、更改)存储在移动装置中的系统参数/数据，以使移动装置相应地进行操作．由确定步骤 304 进行的判断可以多种方式实施．实施该判断的一种方式是扫描该消息，以判断其是否包括表明可访问移动装置的本地服务的标志或其它标识符．另一种方式是开始执行该消息(即，可执行代码)，然后对任何请求都监视该执行，以访问本地服务．

在任何情况下，当确定步骤 304 判断出该消息不请求访问本地服务时，执行传统的消息处理(步骤 306)．传统的消息处理对本领域技术人员是很熟悉的，因此不再对其讨论．在步骤 306 之后，移动装置消息处理 300 返回，以重复确定步骤 302 和其后的步骤，以处理从网络接收的后续的消息．

另一方面，当确定步骤 304 判断出该消息确实请求访问移动装置的本地服务时，在步骤 308 获取该消息的服务标识．通常，服务标识用于识别消息的来源．消息的服务标识可以有多种形式．例如，该服务标识可以是域名、全部或部分通用资源定位器(URL)、因特网协议(IP)地址、电话号码、文本串的形式或上述形式的组合．然而，服务标识可以是消息的一部分，或者可以由移动装置根据移动装置所具有的对该消息的信息/知识而推知．例如，一个消息本身可以不包括任何形式的服务标识，但移动装置可从该消息已与另一个确切含有服务标识的消息链接的事实中推知服务标识．

一旦在步骤 308 中获得了服务标识，则在步骤 310 中将该消息的服务标识与授权的服务标识进行比较．在一个实施例中，授权的服务标识本地存储在移动装置内．在这样的实施例中，授权的服务标识在初始化期间(见图 2)从网络(例如，网关 104)上安全下载．然而，在其它实施例中，一些或所有的授权的服务标识都可以相对于移动装置远程提供，或者由用户通过键盘和显示屏交互输入．

接下来，确定步骤 312 根据在步骤 310 的比较结果，判断是否发现所述

消息的服务标识与授权的服务标识匹配. 当确定步骤 312 判断出没有发现匹配时, 拒绝该消息访问移动装置的本地服务. 这里, 拒绝该消息访问的原因是该消息不能由授权的服务标识来证实. 通过在这种情况下拒绝访问本地服务, 移动装置的本地服务受到保护, 不能接受未授权的访问. 另一方面, 当确定步骤 312 判断出发现了匹配时, 则在步骤 316 中执行该消息(即, 可执行代码), 从而该消息能够访问移动装置的本地服务. 于是, 在步骤 316 中对消息的执行结果是允许访问移动装置的本地服务, 以通过本地服务更新、增加、删除或者更改移动装置中的系统参数/数据. 在步骤 314 和 316 之后, 移动装置消息处理 300 返回, 以重复确定步骤 302 和后续的步骤, 以处理从网络接收的后续的消息.

图 4A 和 4B 是根据本发明的另一个实施例的移动装置消息处理 400 的流程图. 该移动装置消息处理 400 例如是由图 1 所示的移动装置 102 执行的. 再次说明, 消息通常是从网络提供给移动装置的任何数据块, 并具有包括标题部分和主体部分的格式, 该标题部分包括目标信息, 并且该主体部分包括数据信息. 在通过无线规定移动装置的情况下, 消息通常包含要由移动装置上执行的可执行代码. 由移动装置对可执行代码的执行可调用该装置的本地服务, 以进行该移动装置的规定. 在此实施例中, 移动装置通过网关耦合到网络.

移动装置消息处理 400 首先以确定步骤 402 开始, 该步骤判断是否从网关接收了一消息. 该消息来自网络上的一远程服务器(即, 网点), 并通过网关提供给移动装置. 只要确定步骤 402 判断出还没有从网关接收到消息, 则移动装置消息处理 400 等待接收这样的消息. 然而, 一旦已从网络接收到消息, 则移动装置消息处理 400 继续.

一旦移动装置消息处理 400 继续, 则确定步骤 404 判断该消息是否请求本地服务访问. 这里, 确定步骤 404 判断已从网关接收的消息是否请求对移动装置的本地服务的访问. 对本地服务的访问意味着调用移动装置所提供的本地服务, 该访问可以修改(例如, 增加、删除、更改)存储在移动装置中的系统参数/数据, 以使移动装置相应地进行操作. 由确定步骤 404 进行的判断可以多种方式实施. 实施该判断的一种方式是扫描该消息, 以判断其是否包括表明可访问移动装置的本地服务的标志或其它标识符. 例如, 在称为卡片组的 HDML 消息的情况下, 标识符 " device:"可识别对移动装置的本地服务.

实施该判断的另一种方式是开始执行该消息(即，可执行代码)，然后对任何请求都监视该执行，以访问本地服务．下面的例子表示嵌入消息中的编译和链接后的版本:

```
Service_request()
{
    ...
    device:network_change(CDPD, GSM);
    device:reset_retransmission_time(initial_time, subsequent_time[]);
    ...
}
```

该例子中的规定信息请求当前规定在 CDPD 网络中操作的移动装置现在被规定在 GSM 网络中操作，并且该移动装置还规定成在特定时间段转发消息．在这个例子中， Network_change()和 reset_retransmission_time()对应于移动装置的本地服务．

在任何情况下，当确定步骤 404 判断出该消息不请求访问本地服务时，执行传统的消息处理(步骤 406)．传统的消息处理对本领域技术人员是很熟悉的，因此不再对其讨论．在步骤 406 之后，移动装置消息处理 400 返回，以重复确定步骤 402 和其后的步骤，以处理从网关接收的后续的消息．

另一方面，当确定步骤 404 判断出该消息确实请求访问移动装置的本地服务时，在步骤 408 从该消息的标题部分获取该消息的服务标识．这里，从远程服务器到达网关的消息已经在消息的标题部分具有服务标识，或者，在消息送到移动装置之前将服务标识添加到消息的标题部分．在任何一种情况下，移动装置都能够在步骤 408 从消息的标题部分获取消息的服务标识．通常，服务标识用于识别消息的来源．消息的服务标识可以有多种形式．例如，该服务标识可以是域名、全部或部分 URL 、 IP 地址、电话号码、文本串的形式或上述形式的组合．

一旦在步骤 408 中获得了服务标识，则在步骤 410 中选择一适当的访问控制表．提供多个不同的访问控制表的优点是，对不同的本地服务、不同的移动装置或不同的应用程序，访问控制可以不同．例如，访问控制表可以是全球表，或者，访问控制表可以适合于特定的应用程序或本地服务，或它们

的某些组合. 例如, 在 HDML 的情况下, 访问控制表可以提供给每一个本地服务 HDML 卡片组, 并且, 访问控制表可以由 HDML 中的 ACCESSPATH 和 ACCESSDOMAIN 完成.

一旦选择了适当的访问控制表, 则在步骤 412 中将消息的服务标识与该适当的访问控制表中的授权的服务标识进行比较. 在此实施例中, 访问控制表在初始化期间从网关下载后(见图 2)局部存储在移动装置中.

接下来, 确定步骤 414 根据在步骤 412 的比较结果, 判断是否发现所述消息的服务标识与所述适当的访问控制表中的授权的服务标识匹配. 当确定步骤 414 判断出发现匹配时, 确定步骤 416 判断移动装置和远程服务器之间的连接是否安全. 通常, 网关通过检测连接的状态来获知移动装置和网关之间的连接(经无线网络)为安全. 此外, 网关也能够判断网关和远程服务器之间的连接是否为安全. 例如, 可以利用如安全插接层(Secure Sockets Layer, SSL)或安全 HTTP(secure HTTP)协议之类的安全协议来建立连接, 也可以不利用此类协议建立连接. 总之, 可以利用加密或通过使用专用网络而使这些连接安全.

当确定步骤 416 判断出连接安全时, 在步骤 418 中执行消息(即, 可执行代码), 从而该消息能够访问移动装置的本地服务. 在这种情况下, 消息的服务标识(例如, 来源)为授权的, 并且判断连接为安全的, 于是, 允许该消息访问移动装置的本地服务. 这种安全连接防止了非授权的消息作为授权的服务标识产生的消息冒充通过, 并且, 防止了消息在传输期间被截取和更改. 在步骤 418 之后, 移动装置消息处理 400 返回, 以重复确定步骤 402 和后续的步骤, 以处理从网关接收的后续的消息.

另一方面, 当确定步骤 414 判断出没有发现匹配时, 确定步骤 420 判断是否想要远程校验. 如果想要远程校验, 移动装置消息处理 400 从允许的授权中心请求校验(步骤 422). 这里, 允许的授权中心驻留在网络上. 在一个实施例中, 移动装置将请求消息授权的一请求送到允许的授权中心, 然后等待该允许的授权中心的回答. 接下来, 确定步骤 424 判断消息的服务标识是否已由所述的允许的授权中心校验. 如果校验了消息的服务标识, 则处理进到确定步骤 416, 以便当消息的服务标识与所述的适当的访问控制表中的一个项目匹配时, 随后处理该消息. 或者, 当确定步骤 424 判断出允许的授权中心不能校验消息的服务标识时, 拒绝该消息访问移动装置的本地服务(步骤

426). 这里，拒绝该消息访问是因为该消息不能由适当的访问控制表中的授权的服务标识或允许的授权中心来证实. 通过在这种情况下拒绝访问本地服务，移动装置的本地服务受到保护，不接受未授权的访问. 在步骤 426 之后，移动装置消息处理 400 返回，以重复确定步骤 402 及其后的步骤，以处理从网关接收的后续的消息.

此外，当确定步骤 416 判断出连接不安全时，拒绝所述消息访问移动装置的本地服务(步骤 426). 这里，拒绝该消息访问是因为判断出连接不安全. 通过在这种情况下拒绝访问本地服务，移动装置的本地服务受到保护，不接受未授权的访问.

图 5 是根据本发明的一个实施例的网关处理 500 的流程图，该网关处理 500 处理来自移动装置的请求，以从一服务器下载规定信息. 例如，网关处理 500 由图 1 所示的网关 104 执行.

网关处理 500 首先以确定步骤 502 开始. 确定步骤 502 判断是否已从移动装置接收到一请求. 该请求可嵌入发送到远程服务器的消息中，或者独立作为一个消息发送到通过网络耦合到网关的远程服务器. 例如，信息请求可以是诸如可执行代码的数据块. 当确定步骤 502 判断出还没有从移动装置接收到请求时，网关处理 500 等待接收这样的请求. 然而，一旦确定步骤 502 判断出已经从移动装置接收到请求时，网关处理 500 继续.

一旦网关处理 500 有了要处理的请求，则在步骤 504 中将该请求送到远程服务器. 接下来，确定步骤 506 判断是否已从远程服务器接收响应. 这里，网关处理 500 等待接收来自远程服务器的对在步骤 504 中送到远程服务器的请求的响应. 所等待的响应是请求的信息(例如，数据块). 当没有接收到响应时，确定步骤 506 使网关处理 500 等待响应. 然而，经常使用超时状态，以防止网关处理 500 在过量的时间内等待响应的接收. 一旦确定步骤 506 判断出已从远程服务器接收到响应，则在步骤 508 中校验或附加提供该响应的远程服务器的服务标识. 如果已经接收的响应包括一服务标识，该服务标识可以是该服务的来源信息的一部分，则校验该服务标识. 这里，校验可保证响应的服务标识与远程服务器的服务标识相同，其中请求事先发送到该远程服务器. 或者，当接收的响应不包括服务标识时，附加远程服务器的服务标识，其中请求事先发送到该远程服务器. 此外，网关可通过第三方校验或基于验证(authentication)的认证(certificate)来校验远程服务器的服务标识.